



Configuración de una Amazon VPC



INTRODUCCIÓN

Amazon Virtual Private Cloud (Amazon VPC) le brinda la posibilidad de aprovisionar una sección aislada de forma lógica de la nube de Amazon Web Services (AWS) donde puede iniciar recursos de AWS en una red virtual que usted defina.

OBJETIVOS

- Cree una VPC con una subred privada y pública, una puerta de enlace de Internet y una puerta de enlace NAT.
- Configure las tablas de rutas asociadas con subredes para el tráfico local y dirigido a Internet mediante un gateway de Internet y un gateway NAT.
- Inicie un servidor bastión en una subred pública.
- Utilice un servidor bastión para iniciar sesión en una instancia en una subred privada.



TAREA 1

En esta tarea, creara una VPC.

- En la Consola de administración de AWS, en la barra de búsqueda, ingrese y elija VPC ir a la Consola de administración de VPC.
- En el panel de navegación izquierdo, para Nube privada virtual, elija Sus VPC.
- Seleccione Crear VPC y configure las siguientes opciones:

Configuración de la VPC

Recursos que se van a crear [Información](#)
Cree únicamente el recurso de VPC o la VPC y otros recursos de red.

☒ Solo la VPC ☐ VPC y más

Etiqueta de nombre - *opcional*
Crea una etiqueta con una clave de "Nombre" y el valor que usted especifique.

Lab VPC

Bloque de CIDR IPv4 [Información](#)
☒ Entrada manual de CIDR IPv4
☐ Bloque de CIDR IPv4 asignado por IPAM

CIDR IPv4
10.0.0.0/16
El tamaño del bloque CIDR debe estar entre /16 y /28.

Bloque de CIDR IPv6 [Información](#)
☒ Sin bloque de CIDR IPv6
☐ Bloque de CIDR IPv6 asignado por IPAM
☐ Bloque de CIDR IPv6 proporcionado por Amazon
☐ CIDR IPv6 de mi propiedad

Tenencia [Información](#)
Predeterminado ▼

- Seleccione Crear VPC.
- Seleccione Acciones y elija Editar configuración de VPC.



vpc-01657a41aebaaa58a / Lab VPC

Acciones ▴

Crear registro de flujo

Editar la configuración de VPC

Editar los CIDR

Administrar las rutas del dispositivo de red

Administrar etiquetas

Eliminar la VPC

Detalles

Información

ID de la VPC	Estado	Nombres de host de DNS	
 vpc-01657a41aebaaa58a	 Available	Desactivado	
Tenencia	Conjunto de opciones de DHCP	Tabla de enrutamiento prin	
Default	dopt-03c5c2f1ed7ec24a1	rtb-0787010b1a0ce1679	
VPC predeterminada	CIDR IPv4	Grupo IPv6	CIDR IPv6 (grupo de bordes de red)
No	10.0.0.0/16	–	–
Métricas de uso de direcciones de red	Grupos de reglas del firewall de DNS de Route 53 Resolver	ID de propietario	
Desactivado	–	 690855467622	

- En la sección de configuración de DNS, seleccione Habilitar nombres de host DNS.

Configuración de DNS

☒ Habilitar la resolución de DNS

Información

☒ Habilitar nombres de host DNS

Información

- Seleccione Guardar.



TAREA 2

En esta tarea, creará una subred pública y una subred privada.

- En el panel de navegación izquierdo, para Nube privada virtual, elija Subredes.
- Seleccione Crear subred y configure las siguientes opciones:

Configuración de la subred
Especifique los bloques de CIDR y la zona de disponibilidad de la subred.

Subred 1 de 1

Nombre de la subred
Cree una etiqueta con una clave de "Nombre" y el valor que especifique.

El nombre puede tener un máximo de 256 caracteres.

Zona de disponibilidad [Información](#)
Elija la zona en la que residirá la subred o deje que Amazon elija una por usted.

Bloque de CIDR de VPC IPv4 [Información](#)
Elija el bloque CIDR IPv4 de la VPC para la subred. El CIDR IPv4 de la subred debe estar dentro de este bloque.

Bloque de CIDR de la subred IPv4
 256 IPs
< > ^ v

- Seleccione Crear subred.
- Seleccionar subred pública.
- Seleccione Acciones y luego seleccione Editar configuración de subred.

Subredes (1/1) [Información](#)

Find resources by attribute or tag
ID de subred: subnet-0091dd444fe9ca46e

<input checked="" type="checkbox"/>	Name	ID de subred
<input checked="" type="checkbox"/>	Public Subnet	subnet-0091dd444fe9ca46e

Acciones

- Ver detalles
- Crear registro de flujo
- Editar la configuración de la subred**
- Editar CIDR de IPv6
- Editar la asociación de ACL de red
- Editar la asociación de la tabla de enrutamiento
- Editar reservas de CIDR
- Compartir subred
- Administrar etiquetas
- Eliminar subred



- En la sección Configuración de asignación automática de IP, seleccione Habilitar asignación automática de dirección IPv4 pública.

Configuración de la asignación automática de IP [Información](#)

Permita que AWS asigne automáticamente una dirección IPv4 o IPv6 pública a una nueva interfaz de red principal para una instancia de esta subred.

☒ **Habilitar la asignación automática de la dirección IPv4 pública** [Información](#)

☐ **Habilitar la asignación automática de direcciones IPv4 propiedad del cliente**

[Información](#)

Opción desactivada porque no se encontraron grupos propiedad del cliente.

- Seleccione Guardar.
- Para crear la subred privada, repita los pasos de la tarea anterior y elija las siguientes opciones:

Configuración de la subred

Especifique los bloques de CIDR y la zona de disponibilidad de la subred.

Subred 1 de 1

Nombre de la subred

Cree una etiqueta con una clave de "Nombre" y el valor que especifique.

Private Subnet

El nombre puede tener un máximo de 256 caracteres.

Zona de disponibilidad [Información](#)

Elija la zona en la que residirá la subred o deje que Amazon elija una por usted.

Sin preferencia

Bloque de CIDR de VPC IPv4 [Información](#)

Elija el bloque CIDR IPv4 de la VPC para la subred. El CIDR IPv4 de la subred debe estar dentro de este bloque.

10.0.0.0/16

Bloque de CIDR de la subred IPv4

10.0.2.0/23 512 IPs

< > ^ v

- Seleccione Crear subred.



TAREA 3

En esta tarea, creará una puerta de enlace de Internet para su VPC. Necesitará una puerta de enlace de Internet para establecer conectividad externa con instancias EC2 en VPC.

- En el panel de navegación izquierdo, para Nube privada virtual, seleccione Puertas de enlace de Internet.
- Seleccione Crear puerta de enlace de Internet y, a continuación, en Etiqueta de nombre, ingrese Lab IGW.

Configuración de gateway de Internet

Etiqueta de nombre
Crea una etiqueta con una clave de "Nombre" y el valor que usted especifique.

Lab IGW

- Seleccione Crear puerta de enlace de Internet.
- Seleccione Acciones y luego elija Conectar a una VPC.

VPC > Gateways de Internet > igw-0af59b8de95250f38

igw-0af59b8de95250f38 / Lab IGW

Detalles Información

ID de gateway de Internet igw-0af59b8de95250f38	Estado Detached	ID de la VPC -	Propietario 690
--	--------------------	-------------------	--------------------

Acciones ▲
Conectar a la VPC
Desconectar de la VPC
Administrar etiquetas
Eliminar

VPC
Conecte una gateway de Internet a la VPC para habilitar la comunicación con Internet. Especifique la VPC que desea asociar a continuación.

VPC disponibles
Conecte la gateway de Internet a esta VPC.

Q vpc-01657a41aebaaa58a X

► Comando de la interfaz de línea de comandos de AWS



TAREA 4

Ahora está En esta tarea, harás lo siguiente: Cree una tabla de rutas públicas para el tráfico dirigido a Internet. Agregue una ruta a la tabla de rutas para dirigir el tráfico de Internet al portal de Internet. Asocie la subred pública con la nueva tabla de rutas.

- En el panel de navegación izquierdo, para Nube privada virtual, elija Tablas de rutas.
- Seleccione la tabla de rutas que incluye Lab VPC en la columna VPC.
- En la columna Nombre, elija el ícono de edición, ingrese Private Route TableEditar nombre y luego elija Guardar.

The screenshot shows the AWS Management Console interface for 'Tablas de enrutamiento (1/2)'. A modal dialog titled 'Editar Name' is open, allowing the user to edit the name of a selected route table. The input field contains the text 'Private Route Table'. Below the input field are two buttons: 'Cancelar' and 'Guardar'.

Name	ID de tabla de enrutam...	Asociaciones de subre...	Asociaciones de...	Princ...
- [editar]	-0787010b1a0ce1679	-	-	Sí
- [editar]	-015713f8071bd17e8	-	-	Sí

- Seleccione la pestaña Rutas.
- Seleccione Crear tabla de rutas y configure las siguientes opciones:



Configuración de la tabla de enrutamiento

Nombre - *opcional*

Cree una etiqueta con una clave de "Nombre" y el valor que especifique.

Public Route Table

VPC

La VPC que se debe usar para esta tabla de enrutamiento.

vpc-01657a41aebaaa58a (Lab VPC)

- Seleccione Crear tabla de rutas.
- Después de crear la tabla de rutas, en la pestaña Rutas, elija Editar rutas.
- Seleccione Agregar ruta y luego configure las siguientes opciones:

Destino	Destino	Estado	Propagada
10.0.0.0/16	local	Activo	No
Q 0.0.0.0/0	Q local		
	Puerta de enlace de Internet	-	No
	Q igw-0af59b8de95250f38		
<div>Quitar</div>			
<div>Agregar ruta</div>			

- Seleccione Guardar cambios.
- Seleccione la pestaña Asociaciones de subred.
- Seleccione Editar asociaciones de subred.
- Seleccionar subred pública.

Subredes disponibles (1/2)						
Filtrar asociaciones de subredes						
	Nombre	ID de subred	CIDR IPv4	CIDR IPv6	ID de tabla de enrutamiento	
<input checked="" type="checkbox"/>	Public Subnet	subnet-0091dd444fe9ca46e	10.0.0.0/24	-	Principal (rtb-0787010b1a0ce167)	
<input type="checkbox"/>	Private Subnet	subnet-06a68af250a668e23	10.0.2.0/23	-	Principal (rtb-0787010b1a0ce167)	

- Seleccione Guardar asociaciones.



TAREA 5

Un servidor bastión (también conocido como jump box) es una instancia de EC2 en una subred pública que está configurada de forma segura para brindar acceso a recursos en una subred privada. Los operadores de sistemas pueden conectarse al servidor bastión y luego acceder a recursos en la subred privada.

En esta tarea, inicia un servidor bastión de instancia EC2 en la subred pública que creaste anteriormente.

- o En la consola de administración de AWS, en la barra de búsqueda, ingrese y elija EC2ir a la consola de administración de EC2.
- o En el panel de navegación izquierdo, seleccione Instancias.
- o Seleccione Iniciar instancias y configure las siguientes opciones:

Nombre y etiquetas [Información](#)

Nombre

[Agregar etiquetas adicionales](#)



Inicio rápido

Amazon Linux
aws

macOS
Mac

Ubuntu
ubuntu

Windows
Microsoft

Red Hat
Red Hat

SUSE L
SUS

Buscar más AMI
Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)

AMI de Amazon Linux 2023
ami-08d8ac128e0a1b91c (64 bits (x86), uefi-preferred) / ami-03455155bfe406fa1 (64 bits (Arm), uefi)
Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs

Apto para la capa gratuita ▼

▼ Tipo de instancia [Información](#) | [Obtener asesoramiento](#)

Tipo de instancia

t3.micro
Familia: t3 2 vCPU 1 GiB Memoria Generación actual: true
Bajo demanda SUSE base precios: 0.0104 USD por hora
Bajo demanda Windows base precios: 0.0196 USD por hora
Bajo demanda RHEL base precios: 0.0392 USD por hora
Bajo demanda Linux base precios: 0.0104 USD por hora

☒ Todas las generaciones

[Comparar tipos de instancias](#)

Se aplican costos adicionales a las AMI con software preinstalado

▼ Par de claves (inicio de sesión) [Información](#)

Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de que tiene acceso al par de claves seleccionado antes de lanzar la instancia.

Nombre del par de claves - obligatorio

Continuar sin un par de claves (no recomendado) Valor predeterminado ▼

[Crear un nuevo par de claves](#)

▼ Configuraciones de red [Información](#)

VPC: obligatorio [Información](#)

vpc-01657a41aebaaa58a (Lab VPC)
10.0.0.0/16



Subred [Información](#)

subnet-0091dd444fe9ca46e Public Subnet
VPC: vpc-01657a41aebaaa58a Propietario: 690855467622
Zona de disponibilidad: us-west-2d Tipo de zona: Zona de disponibilidad
Direcciones IP disponibles: 251 CIDR: 10.0.0.0/24



[Crear nueva subred](#)

Asignar automáticamente la IP pública [Información](#)

Habilitar

Se aplican cargos adicionales cuando no se cumplen los límites del nivel gratuito



Firewall (grupos de seguridad) | [Información](#)

Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Agregue reglas para permitir que un tráfico específico llegue a la instancia.

☒ Crear grupo de seguridad ☐ Seleccionar un grupo de seguridad existente

Nombre del grupo de seguridad - *obligatorio*

Bastion Security Group

Este grupo de seguridad se agregará a todas las interfaces de red. El nombre no se puede editar después de crear el grupo de seguridad. La longitud máxima es de 255 caracteres. Caracteres válidos: a-z, A-Z, 0-9, espacios y _-:/()#,@!+=&;[]!\$*

Descripción - *obligatorio* | [Información](#)

Allow SSH

Reglas de grupos de seguridad de entrada

▼ Regla del grupo de seguridad 1 (TCP, 22, 0.0.0.0/0) Eliminar

Tipo Información	Protocolo Información	Intervalo de puertos Información
ssh ▼	TCP	22
Tipo de origen Información	Origen Información	Descripción - <i>opcional</i> Información
Cualquier lugar ▼	<input type="text" value="Agregue CIDR, lista de prefijos"/> 0.0.0.0/0 ✕	por ejemplo, SSH para Admin Desk

- o En la sección Configuración de red, elija Editar y configure las siguientes opciones:
- o Seleccione Instancia de lanzamiento.
- o Para mostrar la instancia lanzada, elija Ver todas las instancias.

Instancias (1) | [Información](#)

Última actualización: Hace less than a minute Actualizar Conectar Estado de la instancia ▼ Acciones ▼ Lanzar instancias ▼

Todos los estados ▼ < 1 > ⚙️

<input type="checkbox"/>	Name ✎ ▼	ID de la instancia	Estado de la i... ▼	Tipo de inst... ▼	Comprobación de	Estado de la al...	Zona d
<input type="checkbox"/>	Bastion Server	i-0cd2a55bce65b49b9	En ejecución 🔍	t3.micro	Iniciando	Ver alarmas +	us-wes



TAREA 6

En esta tarea, inicia una puerta de enlace NAT en la subred pública y configura la tabla de rutas privadas para facilitar la comunicación entre los recursos de la subred privada e Internet.

- En la consola de administración de AWS, en la barra de búsqueda, ingrese NAT gateways, elija la lista Características y elija Puertas de enlace NAT.
- Seleccione Crear puerta de enlace NAT y configure las siguientes opciones:
- Seleccione Asignar IP elástica.

Configuración de gateway NAT

Nombre - *opcional*
Cree una etiqueta con una clave de "Nombre" y el valor que especifique.

Lab NAT gateway

El nombre puede tener un máximo de 256 caracteres.

Subred
Seleccione una subred en la que va a crear la gateway NAT.

subnet-0091dd444fe9ca46e (Public Subnet) ▼

Tipo de conectividad
Seleccione un tipo de conectividad para la gateway NAT.

☒ Pública
☐ Privada

ID de asignación de IP elástica [Información](#)
Asigne una dirección IP elástica a la gateway NAT.

eipalloc-0f00d90a92652cd0f ▼

Asignar IP elástica

► Configuraciones adicionales [Información](#)

- Seleccione Crear una puerta de enlace NAT.



- En el panel de navegación izquierdo, elija Tablas de rutas y luego seleccione Tabla de rutas privadas.
- Seleccione la pestaña Rutas.
- Seleccione Editar rutas.
- Seleccione Agregar ruta y configure las siguientes opciones:

Destino	Destino	Estado	Propagada
10.0.0.0/16	<div>local</div>	🟢 Activo	No
<div>Q 0.0.0.0/0</div>	<div>Q local</div>	-	No
	<div>Puerta de enlace NAT</div>		
	<div>Q nat-0a687363b6b602018</div>		
<div>Agregar ruta</div>			

- Seleccione Guardar cambios.